Release A CDR RID Report

Date Last Modified 3/4/96

Originator Hal Folts/Leon Jordan **Phone No** 301 286-3512/301-794-1

Organization ESDIS/CSC

E Mail Address folts@eos.nasa.gov/qjordan@ulabsgi.gsfc.nasa.gov

Document Release A MSS Design Specification (305-CD-013-001)

Section Management Software CSCI, Section 6 **Page** beginning Page 6-1 **Figure Table** N/A

RID ID **CDR** 81
Review Release A CDR
Originator Ref DSNO 6
Priority 2

Category Name MSS Design **Actionee** ECS

Sub Category

Subject Management CSCI Detail

Description of Problem or Suggestion:

(1) Descriptive detail, in terms of textual description and scenarios, is needed for Fault Management to show
- how short versus long term fault information is handled
- how analysis and trending is done
- the interface with Trouble Ticketing
- different levels of fault management activities for the site and SMC.
- list of specific summary data to pass up to SMC from sites.

(2) Descriptive detail, in terms of textual description and scenarios, is needed for Performance Management to show
- how the operator is supported in Performance Management -- e.g., in a situation where performance is degrading and production or productivity is an important issue
- what information presented and how
- what specific performance analysis capabilities are provided
- what performance prediction capabilities are provided • how long versus short term performance information is handled
- different levels of activity between the site and SMC
- list of specific summary data to pass up to SMC from sites
- specific lists of performance metrics for gateways, FDDI links, and Ethernet links.

(3) Descriptive detail, in terms of textual description and scenarios, is needed for Security Management to show
- how different types of security events are detected and handled
- what specific mechanisms are used
- what the criteria for each type of security event are (e.g., how many logon failures constitute an event)
- how security event information is organized, presented, and used
- what capabilities are provided to support analysis and detection of complex security events (e.g., intrusion across sites)
- how intrusion recovery is supported
- levels of security management between the site and SMC

Originator's Recommendation

Supply the requested textual information, lists, and scenarios.

GSFC Response by: **GSFC Response Date**

HAIS Response by: Gary Forman **HAIS Schedule** 9/20/95

HAIS R. E. Lou Swentek **HAIS Response Date** 11/29/95

The specific response to each of the problems listed is addressed below:

(1) Fault management

• The handling of short term vs. long term fault information was not included in the document since the selection of the Fault Management application had not yet been approved. The document will be updated to reflect those capabilities in section 6.1.1.
• Fault analysis and trending information was not included in the document since the selection of the Fault Management application had not yet been approved. The document will be updated to reflect those capabilities in section 6.1.1.
• Although the Trouble Ticketing COTS package (Remedy) is capable of interfacing directly with both of the selected Fault Management applications (HP OpenView and Tivoli), this potential interface will not be implemented in Release A.
• A description of the different levels of Fault Management activities at the SMC and the sites is contained in the operational concepts and operations scenarios documents rather than the detailed design specification, as the same functionality will be provided at both the SMC and sites (the policies associated with the use of that functionality will differ, however). The Fault Management scenario included in DID 605 provides a representative view of the Fault Management activities. All Fault Management operator interfaces will be documented in DID 609/611.
• The document will be updated to reflect specific summary fault data passed to the SMC.

(2) Performance Management

Management operator interfaces will be documented in DID 609/611.
• The document will be updated to reflect specific summary fault data passed to the SMC.

(2) Performance Management

• The support of the operator by Performance Management is contained in the operational concepts and operations scenarios documents.
• The type of information presented to the operator and the actual operator interface are described in the operations scenarios document (DID 605).
• Specific performance analysis capabilities were not included in the document since the selection of the Performance Management application had not yet been approved. The document will be updated to reflect those capabilities in section 6.2.1.
• Performance prediction capabilities were not included in the document since the selection of the Performance Management application had not yet been approved. The document will be updated to reflect those capabilities in section 6.2.1.
• The handling of long term vs. short term information was not included in the document since the selection of the Performance Management application had not yet been approved. The document will be updated to reflect those capabilities in section 6.2.1.
• A description of the different levels of Performance Management activities at the SMC and the sites is contained in the operational concepts and operations scenarios documents rather than the detailed design specification, as the same functionality will be provided at both the SMC and sites (the policies associated with the use of that functionality will differ, however). The Performance Management scenario included in DID 605 provides a representative view of the Performance Management activities. All Performance Management operator interfaces will be documented in DID 609/611.
• The document will be updated to reflect specific summary performance data passed to the SMC.
• The specific lists of performance metrics in DID 305 were intended to provided representative examples of performance metrics. The document will be updated to provide represenative metrics for these managed objects as well.

(3) Security Management

• A table listing the different types of security events and the COTS packages used to detect and handle them will be added to the document in section 6.3.1.
• Brief descriptions of COTS packages and mechanisms used to detect and handle security events will be added to the document in section 6.3.1. Specific details regarding the mechanisms used by the COTS packages are provided in vendor documentation.
• The criteria used to define each type of security event (such as how many login failures constitutes an event) is a policy issue, not a design issue. The MSS is designed to be configurable so that the criteria can be changed to meet whatever security policy is set by ESDIS.
• The Security Management scenario included in DID 605 provides a representative view of the organization, presentation, and use of security event data. The organization, presentation, and use of all security event data will be documented in DID 609/611.
• Analysis and detection of intrusions across DAACs will be performed at the SMC through the use of the MsScSMC class. As mentioned above, the criteria used to define these events will be based on ESDIS security policy.
• Intrusion recovery is supported through the use of backup and restore procedures described in DID 605.
• A description of the different levels of Security Management activities at the SMC and the sites is contained in the operational concepts and operations scenarios documents rather than the detailed design specification, as the same functionality will be provided at both the SMC and sites (the policies associated with the use of that functionality will differ, however). The Security Management scenario included in DID 605 provides a representative view of the Security Management activities. All Security Management activities will be documented in DID 609/611.
• The document will be updated to reflect specific summary performance data passed to the SMC.
• User activity history will be analyzed to detect security events. Some of the events captured in this history, such as events for invalid password, will be captured in event logs as security events. Therefore, although it uses the same logging mechanism and the same logs as those used by Accountability Management, Security Management will not interface directly with Accountabilty Management. As mentioned above, the details as to what constitutes a security event are matters of ESDIS security policy. MSS will be capable of enforcing those policies as defined.

(4) Accountability Management

• The document will be updated to reflect user activity data.
• The document will be updated to include information on activities associated with a data item.
• The document will be updated to reflect audit activity.
• The document will be updated to reflect data processing information retrieval.
• The document will be updated to reflect ordered item status data (including values).
• Transactions associated with a particular user are entered into the accountability database upon the successful completion of the transaction. Therefore, there is no need to back out transactions.
• There is no interface between Accountability Management and Fault Management or Security Management.
• Some of the fields included in the user profile will be used by the future billing capability.
• A description of the different levels of Accountability Management activities at the SMC and the sites is contained in the operational concepts and operations scenarios documents rather than the detailed design specification, as the same functionality will be provided at both the SMC and sites (the policies associated with the use of that functionality will differ, however). The Accountability Management scenario included in DID 605 provides a representative view of the Accountability Management activities. All Accountability Management activities will be documented in DID 609/611.
• The document will be updated to reflect specific summary performance data passed to the SMC.

Release A CDR RID Report

Status **Closed** **Date Closed** **3/4/96** **Sponsor** **Folts**

****** **Attachment if any** ******